UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,794	04/27/2001	Carter Shanklin	CAPTNE/P005A1	2564

29914 7590 08/12/2004

DKW LAW GROUP, P.C.
58TH FLOOR - USX TOWER
600 GRANT STREET
PITTSBURGH, PA 15219

EXAMINER	
OSMAN, RAMY M	
ART UNIT	**PAPER NUMBER**
2157	

DATE MAILED: 08/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/844,794	SHANKLIN ET AL.	
	Examiner	Art Unit	
	Ramy M Osman	2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☒ Claim(s) *12 and 13* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 April 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to because the figures are of poor quality with some of them being unreadable. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

2. A series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

Claims 12 and 13 are objected.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 4 and 5 recite the limitation "the firewall device" in lines 17 and 22. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

6. Claims 1,2,4,5,14,15 and 17 rejected under 35 U.S.C. 102(a) as being anticipated by Hill et al. (US Patent No 6,088,804).

7. In reference to claims 1 and 15, Hill teaches a method of protecting a network from potentially harmful data traffic traversing a plurality of data ports of the network, the data traffic comprising data packets (Abstract and figure 1), the method comprising the steps of:

a. providing a means for monitoring attributes of data traffic traversing a plurality of data ports of a network (Summary and column 1 lines 5-10);

b. providing a means for responding when an attack on said network is determined to occur (Summary and column 1 lines 5-10);

c. defining a set of attack parameters from attributes of one or more data packets traversing a network, such that when said defined set of parameters are met an attack on said network is presumed to occur (column 2 line 63 – column 3 line 16);

d. specifying a set of responses that may be taken in response to said attack, wherein said responses are defined by said response rules being designed to select one or more of said responses from said set of specified responses based upon monitored attack parameters (column 3 lines 7-15 and lines 25-40, column 7 line 45 – column 8 line 60 and column 9 lines 45-67);

e. monitoring all the data packets traversing the data ports from a plurality of sources with said monitoring means to determine when said attack parameters have been met (Abstract, figure 1 and column 4 lines 11-55);

f. comparing and coordinating said attack parameters and said response rules to select one or more of said set of specified responses based upon said monitored attack parameters (column 3 lines 7-15 and lines 25-40, column 7 line 45 – column 8 line 60 and column 9 lines 45-67); and

g. providing said one or more selected responses through said response providing means to protect said network from said attack (column 1 lines 5-10 and column 3 lines 17-40).

8. In reference to claims 2 and 17, Hill teaches the method of claim 1 wherein said set of responses is selected from the of access response, an alert response wherein an alert of said attack is provided, a throttling response wherein data packets are queued and sent along the network at a controlled rate, a redirection response wherein the attack from an attacking source is redirected to another destination, and combinations thereof (column 5 lines 25-67).

9. In reference to claim 4, Hill teaches the method of claim 1, wherein said means monitoring attributes of data traffic traversing a plurality of data ports of a network is through non-promiscuous packet capturing on the firewall device (column 4 lines 40-60).

10. In reference to claim 5, Hill teaches the method of claim 1, wherein said means for responding when an attack on said network is determined to control rules on the firewall device (column 5 line 35 – column 6 line 20).

11. In reference to claim 14, Hill teaches the method of claim 1, wherein said response rules are user defined (Abstract and Summary).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 3 and 18 rejected under 35 U.S.C. 103(a) as being unpatentable over Hill et al (US Patent No 6,088,804) in view of Stone (US Patent No 5,546,390).

Hill teaches the method of claim 1 above which includes comparing and coordinating said attack parameters and said response rules (Summary and column 5 lines 25-67). Hill fails to explicitly teach utilizing a Radix tree. However, Radix tree is well known in the art comparison and decision methods and is taught by Stone (column 5 lines 20-67 and column 9 lines 45-67).

14. Claims 6-13,16 and 19-21 rejected under 35 U.S.C. 103(a) as being unpatentable over Hill et al (US Patent No 6,088,804) in view of Cunningham et al (US Patent No 6,219,786).

15. In reference to claims 6,7 and 16, Hill fails to explicitly teach wherein said attributes of said data packets are selected from the group consisting of a data packet's source address, a data packet's destination address, a data packet's source port, the number of data packets from a source address per time; the number of data packets from a source port per unit of time, a data packet's protocol, and combinations thereof. However, Cunningham teaches analyzing packet attributes from a group of consisting of source and destination address/port, number of packets and packet protocol, for the

purpose of monitoring and controlling network access for network security (column 3 lines 20-55 and column 6 line 49 – column 7 line 55).

It would have been obvious for one of ordinary skill in the art to modify Hill by making the data attributes packet attributes consisting of a data packet's source address, a data packet's destination address, a data packet's source port, the number of data packets from a source address per time; the number of data packets from a source port per unit of time, a data packet's protocol as per the teachings of Cunningham so that network access can be monitored and controlled for network security.

16. In reference to claim 8, Hill teaches the method of claim 2 above. Hill fails to explicitly teach wherein the step denying access to the source is automatic. However, Cunningham teaches automatically denying access to the source, for the purpose of controlling network access for network security (column 8 line 54 – column 9 line 16).

It would have been obvious for one of ordinary skill in the art to modify Hill by making the step denying access to the source as automatic as per the teachings of Cunningham for controlling network access for network security.

17. In reference to claim 9, Hill teaches the method of claim 1 above. Hill fails to explicitly teach claim 1 further comprising step of copying each of the data packets for monitoring. However, Cunningham teaches storing the data for monitoring (column 7 line 56 – column 8 line 35).

It would have been obvious for one of ordinary skill in the art to modify Hill by copying each of the data packets for monitoring as per the teachings of Cunningham for the purpose of data monitoring for network security.

18. In reference to claim 10, Hill teaches the method of claim 1 above. Hill fails to explicitly teach wherein the step monitoring further comprises monitoring both incoming and outgoing data packets traversing the data ports. However, Cunningham teaches monitoring incoming and outgoing connections (column 4 lines 31-44).

It would have been obvious for one of ordinary skill in the art to modify Hill by monitoring incoming and outgoing connections as per the teachings of Cunningham for controlling network access for network security.

19. In reference to claim 11, Hill teaches the method of claim 1 above. Hill fails to explicitly teach where the step of monitoring further comprises separately monitoring the data packets traversing each of the data ports. However, Cunningham teaches separately monitoring packets on ports (column 2 lines 45-67 and column 10 lines 1-51).

It would have been obvious for one of ordinary skill in the art to modify Hill by separately monitoring packets on ports as per the teachings of Cunningham for controlling network access for network security.

20. In reference to claim 12, Hill teaches the method of claim 2 above. Hill fails to explicitly teach wherein further comprising allowing data packets from sources other than the denied source to traverse the data ports. However, Cunningham teaches allowing data packets from sources other than the denied source to traverse the data ports (column 3 line 56 – column 4 line 16, column 6 lines 49-67 and column 7 lines 1-15).

It would have been obvious for one of ordinary skill in the art to modify Hill by allowing data packets from sources other than the denied source to traverse the data ports as per the teachings of Cunningham for controlling network access for network security.

21. In reference to claim 13, Hill teaches the method of claim 2 above. Hill fails to explicitly teach wherein further comprising allowing packets from protocols other than the denied protocol to traverse the data ports. However, Cunningham teaches allowing packets from protocols other than the denied protocol to traverse the data ports (column 6 lines 49-67 and column 9 lines 1-20).

It would have been obvious for one of ordinary skill in the art to modify Hill by allowing packets from protocols other than the denied protocol to traverse the data ports as per the teachings of Cunningham for controlling network access for network security.

22. In reference to claims 19 and 20, Hill teaches the method of claim 15 above. Hill fails to explicitly teach wherein said data monitoring means, said memory and said processor are contained within a router. However, Cunningham teaches monitoring through a router (column 2 lines 30-60 and column 5 lines 5-25).

It would have been obvious for one of ordinary skill in the art to modify Hill by monitoring through a router as per the teachings of Cunningham for controlling network access for network security.

23. In reference to claim 21, Hill teaches the method of claim 20 above. Hill fails to explicitly teach wherein said router is used in combination with a computer firewall. However, Cunningham teaches a router combined with firewall technology (column 2 lines 30-60 and column 5 lines 5-25).

It would have been obvious for one of ordinary skill in the art to modify Hill wherein said router is used in combination with a computer firewall as per the teachings of Cunningham for controlling network access for network security.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ramy M Osman whose telephone number is (703) 305-8050. The examiner can normally be reached on M-F 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (703) 308-7562. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RMO
August 4, 2004

SALEH NAJJAR
PRIMARY EXAMINER